

🔍 Title: **CN1211770A: HUMAN BODY PHYSIOLOGICAL CHARACTERISTICS ANTIFAKE VERIFICATION METHOD CORRELATED WITH IDENTIFICATION CARD MOBILE DATA BASE**

🔍 Derwent Title: Human body physiological characteristics antifake verification method correlated with identification card mobile data base - uses physiological characteristics information, personal economic bill and personal archives of the certificate card owner
[\[Derwent Record\]](#)

🔍 Country: **CN** China
🔍 Kind: **A** Unexamined APPLIC. open to Public inspection ⁱ

🔍 Inventor: **ZHENNING YANG**; China

🔍 Assignee: **YANG ZHENNING** China
[News, Profiles, Stocks and More about this company](#)



High
Resolution

🔍 Published / Filed: **1999-03-24** / 1998-03-27

🔍 Application Number: **CN19981998981119**

🔍 IPC Code: Advanced: **G06F 17/30**;
Core: more...
IPC-7: **G06F 17/30**;

🔍 ECLA Code: None

🔍 Priority Number: 1998-03-27 **CN1998199898111909**

🔍 Abstract: An antiforge authentication method for certificate card features that the physiological characteristics information, personal economic bill and personal archives of the certificate card owner are acquired, digitalized, compressed and encrypted to create a mobile database of the certificate card. When the certificate card is scanned, the forge card can be judged based on if the physiological characteristics of its holder is matched with that of owner. The number of users is not limited in network.

🔍 Family:

PDF	Publication	Pub. Date	Filed	Title
	CN1211770A	1999-03-24	1998-03-27	HUMAN BODY PHYSIOLOGICAL CHARACTERISTICS ANTIFAKE VERIFICATION METHOD CORRELATED WITH IDENTIFICATION CARD MOBILE DATA BASE
1 family members shown above				

🔍 Other Abstract Info: None

[19]中华人民共和国国家知识产权局

[51]Int. Cl⁶
G06F 17/30

[12] 发明专利申请公开说明书

[21] 申请号 98111909.3

[43]公开日 1999 年 3 月 24 日

[11]公开号 CN 1211770A

[22]申请日 98.3.27 [21]申请号 98111909.3
[71]申请人 杨振宁
地址 610041 四川省成都市人民南路三段三号成都气象学院科研所
[72]发明人 杨振宁

权利要求书 2 页 说明书 12 页 附图页数 11 页

[54]发明名称 人体生理特征与识别卡流动数据库互相关
防伪认证法

[57]摘要

一种识别卡防伪认证法;使用户通过采集申请识别卡者人体生理特征信息或包括个人财务帐单或包括个人档案并将其数码化后,再经压缩和加密处理共同构成识别卡流动数据库;刷卡时,识别卡鉴别与认证持卡者与识别卡流动数据库 人体生理特征信息是否相符?从而达到识别卡防伪造和防伪冒目的以及识别卡 网络用户数不受限制和可脱离网络处理等特点。

ISSN 1 0 0 8 - 4 2 7 4

权 利 要 求 书

1. 一种识别卡防伪认证法；使用户将申请识别卡者人体生理特征和个人财务帐单和个人档案等信息存储入识别卡中从而构成识别卡流动数据库；应用时，当持卡者与识别卡流动数据库间人体生理特征信息经鉴别与认证相符后，识别卡才准许对其进行相关操作；该方法包含：

一个人体生理特征实时采集装置；用户使用数码摄像设备或图像扫描设备采集申请识别卡者的人脸图像、指纹、手几何形态等人体生理特征数码流；

一个人体生理特征数码压缩装置；用户使用二值图像数据压缩算法和静止图像数据压缩算法将人体生理特征数码流压缩成人体生理特征数码压缩流；

一个人体生理特征数码加密装置；用户选择对称或非对称数据加密算法将人体生理特征数码压缩流加密成人体生理特征密码流；

一个识别卡流动数据库；M 个 ($1 \leq M < \infty$) 识别卡流动数据库映射成识别卡数据库中心；

一个识别卡解密装置；该装置采用相应的数据解密算法将人体生理特征密码流解密成人体生理特征数码压缩流；

一个识别卡解压缩装置；该装置采用图像数据解压缩算法将人体生理特征数码压缩流解压缩成人体生理特征数码流；

一个识别卡人体生理特征鉴别与认证装置；该装置采用互相关匹配法或最小绝对差匹配法鉴别与认证两人体生理特征数码流间的相关性；

2. 根据权利要求 1 的识别卡防伪认证法，其特征在于，所述识别卡流动数据库中存储的人体生理特征包括人脸图像或还包括指纹或还包括手几何形态。

3. 根据权利要求 2 的识别卡防伪认证法，其特征在于，所述人体生理特征既可以由人脸照片、指纹照片、手几何形态照片经图像扫描仪扫描后获得，也可直接用数码摄像设备对其数码摄像获得。

4. 根据权利要求 1 的识别卡防伪认证法，其特征在于，所述个人财务帐单记录和描述卡所有者的金融财务状况，如金融余额、流水帐、信用等级、最大允许透支额等信息；

5. 根据权利要求 4 的识别卡防伪认证法，其特征在于，所述个人财务帐单存储入识别卡时需对其经数据压缩算法和数据加密算法处理成个人财务帐单密码

流;

6. 根据权利要求 1 的识别卡防伪认证法, 其特征在于, 所述个人档案记录识别卡所有者的如姓名、性别、出生年月日、住址、民族、籍贯、处分、刑事记录等信息;

7. 根据权利要求 6 的识别卡防伪认证法, 其特征在于, 所述个人档案存储入识别卡时需对其经数据压缩算法和数据加密算法处理成个人档案密码流;

8. 一种识别卡防伪认证法; 使用户将申请识别卡者人体生理特征信息存储入识别卡中从而构成识别卡人体生理特征流动数据库; 应用时, 当持卡者与识别卡流动数据库间人体生理特征信息经鉴别与认证相符后, 识别卡才准许对其进行相关操作; 该方法包含:

一个人体生理特征实时采集装置; 用户使用数码摄像设备或图像扫描设备采集申请识别卡者的人脸图像、指纹、手几何形态等人体生理特征数码流;

一个人体生理特征数码压缩装置; 用户使用二值图像数据压缩算法和静止图像数据压缩算法将人体生理特征数码流压缩成人体生理特征数码压缩流;

一个人体生理特征数码加密装置; 用户选择对称或非对称数据加密算法将人体生理特征数码压缩流加密成人体生理特征密码流;

一个识别卡流动数据库; M 个 ($1 \leq M < \infty$) 识别卡流动数据库映射成识别卡数据库中心;

一个识别卡解密装置; 该装置采用相应的数据解密算法将人体生理特征密码流解密成人体生理特征数码压缩流;

一个识别卡解压缩装置; 该装置采用图像数据解压缩算法将人体生理特征数码压缩流解压缩成人体生理特征数码流;

一个识别卡人体生理特征鉴别与认证装置; 该装置采用互相关匹配法或最小绝对差匹配法鉴别与认证两人体生理特征数码流间的相关性;

人体生理特征与识别卡流动数据库互相关防伪认证法

本发明涉及一种识别卡防伪认证方法，特别是涉及一种识别卡通过互相关验证持卡者人体生理特征与识别卡流动数据库所存人体生理特征映射关系对持卡者身份验证以及识别卡与识别卡网络系统防伪认证的装置和方法。

随着货币电子化进程的不断深化与发展，各类识别卡如信用卡、储蓄卡以及各类磁卡、IC 卡、光卡等在金融和非金融领域里将日益得到广泛应用和普及。但是，人们在享受持卡走遍天下的同时，也担心着一旦识别卡被盗窃或被遗失或被伪造，都将可能产生他人持有该卡进行消费、提款、结算或其他的行为，不但给卡的所有者带来经济和名誉上的损失，也将给发卡机构带来经济和名誉上的损失；导致上述原因在于：

1. 传统的识别卡及其网络系统必须构造识别卡数据库中心

据不完全统计，1997 年涉及识别卡犯罪案件的 60%属内外勾结作案，这是由于识别卡数据库中心的数据结构和数据存储形式导致的必然结果；

案例 1. 某地银行长城卡数据库由于卡号及 PIN 码被盗取后，发生多起利用伪冒长城卡盗取合法客户钱币的案件；

2. 识别卡防伪性

目前我国识别卡应用领域防伪性能最完善的属于指纹储蓄系统，但由于指纹储蓄系统需建立指纹数据库中心，所以其安全性不强；

案例 2. 某地银行应用北京某著名大学的指纹储蓄系统后，由于指纹数据库中指纹被替换，而导致该储户的钱币被他人窃取案件；

3. 识别卡与持卡者间防伪认证性

由于涉及识别卡金融服务的数据基本存储于识别卡数据库中心，识别卡本身的防伪性能未得到足够重视，从而导致涉及伪造和伪冒识别卡犯罪案件呈逐年上升趋势；

案例 3. 某地银行牡丹卡，由于作案嫌疑人利用伪造身份证申请牡丹卡后，进行恶意透支达数十万元；

4. 通讯保密性

原则上, 只要涉及识别卡金融服务的主要数据必需经通讯传输与识别卡数据库中心交换或认证, 则必然存在泄密或被攻击的可能性;

案例 4. 某地银行 ATM 自动提款机由于通讯线路被窃听, 导致犯罪嫌疑人利用窥视提款人密码并伪造储蓄卡后, 恶意提款案件;

5. 如果识别卡核对认证过程必须通过访问近程或远程人体生理特征数据库中心完成, 当所面向的用户群足够大时, 网络系统及其通讯、计算等支持环境的投资必将呈非线性上升趋势, 而面向用户的服务指标却呈现下降趋势; 且当识别卡用户群超过百万数时, 现有网络系统及其通讯、计算等支撑环境将不能确保识别卡业务正常进行; 如某指纹储蓄系统所支持极限用户数为小于百万户。

所以, 有必要提出一种通过: 通过实时采集持卡者人脸图像、指纹、手几何形态等综合人体生理特征信息并转换成人体生理特征数码流, 再经压缩和加密处理成人体生理特征密码流后存储于识别卡内, 从而构造识别卡人体生理特征流动数据库或与个人财务帐单、个人档案等共同构造识别卡流动数据库; 应用时, 持卡者人体生理特征必须与识别卡所存人体生理特征相符且金融服务在识别卡个人财务帐单允许范围时, 方允许完成刷卡过程的识别卡防伪认证方法。

本发明的目的: 通过将持卡者人脸图像、指纹、手几何形态等综合人体生理特征信息数码化后, 经压缩和加密处理成人体生理特征密码流存储入 IC 卡 (Integrated Circuit Card) 或 IC 卡 (Laser Card); 或与个人财务帐单或与个人档案等个人信息共同存储入 IC 卡或 LC 卡中构成识别卡流动数据库; 当持卡者进行消费、提款、结算或身份认证等行为时, 识别卡终端不但核实有关识别卡的原标识信息等, 还将由识别卡进一步鉴别与认证持卡者与识别卡流动数据库中所存人体生理特征信息的相关性, 从而达到识别卡及其应用过程中的防伪造、防变造、防伪冒与认证的目的; 本发明的目的还在于: 通过人体生理特征数码压缩装置采用二值图像数据压缩标准和静止图像数据压缩标准对人体生理特征数码流进行压缩处理, 目的在于减少识别卡网络系统投资和降低识别卡成本; 本发明的目的还在于: 采用对称密码体制或非对称密码体制的数据加密算法, 将人体生理特征数码压缩流经加密处理成人体生理特征密码流并写入识别卡中, 刷卡时由识别卡数据解密算法对其进行解密, 从而使得识别卡中所存人体生理特征信息不能被仿制或假冒。在本发明中, 识别卡储存人体生理特征密码流后构成识别卡人体生理特

征流动数据库，当识别卡网络系统包含有限识别卡群 M ($1 \leq M < \infty$) 时，其人体生理特征数据库中心可映射为 M 个人体生理特征流动数据库，即识别卡网络系统的人体生理特征数据库中心可由 M 个人体生理特征流动数据库替代；同样，包含个人财务帐单或个人档案的 M 个识别卡流动数据库也可替代识别卡数据库中心，从而防止内外勾结作案方式的发生并使得本发明可利用现有的计算环境、网络环境、通讯环境实现；应用时，识别卡与持卡者之间的人体生理特征相关性由识别卡网络终端与识别卡本地化鉴别与认证，而不必访问近程或远程人体生理特征数据库中心，对持卡者金融服务如消费、提款、结算或身份认证等也可仅由识别卡流动数据库和识别卡终端本地化完成；因此，本发明所述识别卡可利用现有计算机网络系统实现且识别卡网络用户数不受限制，是否需要建立人体生理特征数据库完全由发卡机构决定，从而保护了发卡机构的原有投资，并具有识别卡网络系统实现简单化和识别卡网络系统不受用户数限制以及该识别卡安全性和防伪造、防变造、防伪冒性能极强等特点。

本发明所述的人体生理特征数码流既可通过照像后用图像扫描仪扫描获得，也可以通过人体生理特征采集装置如数码摄像设备、活体指纹采集装置和活体手几何形态采集装置获得。通过人体生理特征采集装置采集人体生理特征数码流的方式，一方面可以在自然人或法人申请识别卡时完成，另一方面保证了所采集人体生理特征的实时性和真实性；当该识别卡所有者的人体生理特征因为特殊原因(如车祸、损伤等)而改变时，可以方便地在发卡机构通过人体生理特征采集装置来对其修改；所采集的人体生理特征数码流首先需通过人体生理特征数码压缩装置对其进行压缩处理，以降低识别卡成本和识别卡网络系统设备的投资，所采用的图像数据压缩算法可根据使用者需要选择对称编解码方式或非对称编解码方式；为了保证识别卡所存人体生理特征信息的安全性，写入识别卡前还需通过人体生理特征加密装置对其加密处理成人体生理特征密码流，用于加密处理的数据加密算法可根据使用者需要选择对称数据加密算法或非对称数据加密算法；人体生理特征密码流写入识别卡后，构造成识别卡人体生理特征流动数据库，若与个人财务帐单或个人档案等信息共同写入识别卡中，则构造成识别卡流动数据库；应用时，识别卡内置卡操作系统将会自动根据相应的解密算法及密钥对所存

的人体生理特征密码流进行解密运算并还原成人体生理特征数码压缩流，再经人体生理特征解压缩装置将其解压缩并还原成人体生理特征数码流。

本发明所述的人体生理特征与识别卡流动数据库互相关防伪认证法逻辑流程为：

- 1.首先通过人体生理特征采集装置采集持卡者人脸图像、指纹和手几何形态等人体生理特征信息并转换成人体生理特征数码流；

- 2.再通过二值图像数据压缩算法和静止图像数据压缩算法将其压缩处理成人体生理特征数码压缩流；

- 3.再经对称密码体制或非对称密码体制数据加密算法将其加密处理成人体生理特征密码流后储存到识别卡中，构成识别卡人体生理特征流动数据库；

- 4.识别卡中还可写入个人财务帐单或个人档案等信息后，与人体生理特征信息共同构成识别卡流动数据库；为了降低成本和确保信息的安全，应对个人财务帐单或个人档案经压缩并加密后再储存；

应用时，识别卡网络终端和识别卡鉴别与认证逻辑流程

1. 识别卡网络终端实时采集持卡者人体生理特征并向识别卡发出请求认证信息；

2. 识别卡接受请求认证信息后，读取识别卡网络终端所采集的人体生理特征数码流并采用相应的同密码体制数据解密算法对人体生理特征密码流解密成人体生理特征数码压缩流，再采用与图像数据压缩算法互为映射关系的图像数据解压缩算法将其解压缩并还原成人体生理特征数码流；

3. 识别卡内置人体生理特征鉴别与认证装置对上述两人体生理特征数码流采用互相关匹配法或最小绝对差匹配法进行鉴别与认证，并将认证结果传递至识别卡网络终端；

4. 持卡者与识别卡经鉴别认证相符后，识别卡网络终端根据识别卡个人财务帐单允许范围或个人档案完成相应的刷卡操作，如提款、消费或身份认证等；或识别卡接受对个人财务帐单或个人档案等操作，如修改个人财务帐单或个人档案等；

5. 如需对识别卡进行存款或结算或需修改人体生理特征信息等操作，为了

确保万无一失最好由发卡机构进行或由发卡机构授权机构进行。

本发明所述的人体生理特征与识别卡流动数据库互相关防伪认证法主要步骤描述如下：

1. 人体生理特征数码流的采集

当自然人或法人申请识别卡时，人体生理特征采集装置实时采集识别卡法定持有者的人体生理特征信息；

2. 人体生理特征数码流的压缩

如果所采集的人体生理特征数码流不经压缩存入识别卡则会使得投资过大或者使得识别卡的成本增大，因此，必须对其进行压缩处理。识别卡数码压缩装置将所采集的人体生理特征数码流压缩处理成人体生理特征数码压缩流；该装置所采用的图像数据压缩算法符合二值图像数据压缩标准或符合联合图片专家组——J P E G的静止图像压缩标准；

3. 人体生理特征数码压缩流的加密

不论人体生理特征数码流是否经压缩处理，如果原样存入识别卡是不能有效保密和防伪的。人体生理特征加密装置根据应用环境可选择对称或非对称密码体制的数据加密算法，对经压缩处理后的人体生理特征数码压缩流进行加密处理成人体生理特征密码流。由于，该装置的数据加密算法所用的加密密钥是对他人保密的，所以，他人是很难破译和攻击的；

4. 人体生理特征密码流的储存

将加密处理所得的人体生理特征密码流存入识别卡数码储存装置，如 IC 卡基的存储器或 LC 卡基的光刻区，该存储器读写操作或该光刻区读操作受控于识别卡中卡操作系统(Chip Operation System)，该操作系统中包含加密过程的逆过程——数据解密算法；由于解密密钥存于识别卡中，非发卡机构是不能读取和改写的；除非授权，非发卡机构是不能对识别卡内所存人体生理特征或个人财务帐单或个人档案进行修改的；从而保证识别卡的安全性；

5. 个人财务帐单、个人档案等信息储存

识别卡中可附个人财务帐单，如存款余额、最大透支限额、流水帐等，个人财务帐单数据也将被加密储存；识别卡也可根据应用需要储存个人档案信息；可

擦写信息被储存在 IC 卡电擦写存储器中或 IC 复合卡电擦写存储器中；

6. 人体生理特征密码流的解密

刷卡时，由识别卡网络终端设备向识别卡发出读卡请求，识别卡接到该请求信号并核对无误后，由识别卡解密装置用与人体生理特征加密装置同密码体制的解密算法对所存人体生理特征密码流进行解密处理成人体生理特征数码压缩流；

7. 人体生理特征数码压缩流的解压缩

解密后所得到的人体生理特征数码压缩流输出至识别卡解压缩装置；该装置采用与人体生理特征压缩装置相对应的数据解压缩算法对人体生理特征数码压缩流解压缩处理并还原成人体生理特征数码流；

8. 人体生理特征数码流的显示与传输

解读后的原人体生理特征数码流通过特定传输接口设备或读卡设备传送至图像显示设备或识别卡鉴别与认证装置；图像显示设备按约定的显示方式显示人体生理特征，如人脸图像、指纹、手几何形态等；

9. 人体生理特征实时采集装置

当持卡人刷卡时，面向人脸图像、活体指纹、活体手几何形态等的人体生理特征采集装置将根据应用需要实时采集人体生理特征信息，人体生理特征采集装置由人脸图像摄像装置、活体指纹采集装置、活体手几何形态采集装置等组成；

10. 人体生理特征鉴别与认证装置

人体生理特征鉴别与认证装置接受来自人体生理特征采集装置和识别卡的人体生理特征后，对两者进行重叠覆盖法或自相关法鉴别手段对其认证；从而导致具体应用本发明的过程简化至鉴别与认证本地化和实时化，且无须建立近程或远程人体生理特征中心数据库；

11. 识别卡的应用

根据应用需要，识别卡鉴别与认证时，可选择：(1)单一的人体生理特征识别卡应用法：仅提取识别卡和持卡者的人脸图像或指纹或手几何形态等信息相关鉴别与认证，此类典型应用如代表证用人脸图像识别卡与人眼鉴别认证，一般门禁系统用指纹识别卡与活体指纹采集装置等；(2)可选择两两组合的人体生理特征

识别卡应用法：如选择人脸图像和指纹应用于高级门禁系统时，只有持卡者的人脸图像和指纹与识别卡内所存人脸图像和指纹完全相符时，才准以通过；(3)人脸图像、指纹和手几何形态综合人体生理特征信息的识别卡应用法及范围：原则上，该类识别卡可应用于所有需要防伪或认证领域，尤其是本发明所述的人体生理特征与识别卡相关防伪认证法通过识别卡构成流动的人体生理特征数据库，所以，应用时可不必建立人体生理特征数据库中心，因此，即使拥有亿万用户的应用系统，也仅利用现有计算机环境、网络环境、通讯环境就可实现；(4)当识别卡中储存个人财务帐单后，将使得识别卡作为信用卡或电子货币应用时安全可靠，从而基本杜绝恶意透支等涉及金融犯罪案件的发生；(5)当识别卡中储存个人档案后，将较好解决身份证或护照被伪造或被仿冒等问题。

在上面所述的本发明内容中以及本发明的应用过程中，用于人体生理特征数码流的图像数据压缩算法及其数据格式符合二值图像压缩标准 ISO DIS 11544 和 JPEG 静止图像压缩标准:ISO DIS 10918 | CCITT Recommendation T.81；用于数据加密所用的对称密码体制或非对称密码体制的数据加密算法符合国际数据加密标准或我国《计算机信息系统安全专用产品》标准；识别卡采用 IC 卡 ISO 7816 标准或光卡 ISO/IEC 11693 标准制备；本发明所述数据传输设备和图像显示设备符合 IEEE 接口设备标准和显示设备标准。

本发明的识别卡及其防伪认证方法与前述现有的同类防伪认证方法相比，具有以下特点：

1. 通过构造识别卡人体生理特征流动数据库，使得识别卡及其网络系统应用时不必访问近程或远程人体生理特征数据库中心，从而实现识别卡本地化鉴别与认证，并使得应用本发明可不必设立人体生理特征数据库中心和利用现有计算环境、通讯环境、网络环境实现；

2. 识别卡人体生理特征流动数据库的数据存储形式为密码，其解密受控于识别卡及解密密钥，因此，人体生理特征流动数据库安全性极强，可有效地低御任何非法攻击或破译，从而确保识别卡的安全性；

3. 识别卡人体生理特征流动数据库不但包含人脸图像，还包含指纹和手几何形态等人体表面测量信息，可有效抵御非法攻击者采用仿生医学技术的攻击，因

此，不但使得识别卡的应用范围更广，而且识别卡的整体防伪造、防伪冒性能极强；

4. 识别卡人体生理特征数据库中所存储数据经压缩处理，因此，应用时将减低识别卡成本；

5. 识别卡流动数据库存储个人财务帐单时，不但防伪造和防伪冒性能极强，而且具有可脱机处理的特点，例如当识别卡作为信用卡应用时，即使信用卡特约服务网点没有连网或因故障不能连网也可完成刷卡过程；

6. 识别卡流动数据库存储个人档案时，不但防伪造和防伪冒性能极强，而且具有可脱离网络处理的特点，例如当识别卡作为身份证应用时，即可连网认证也可脱离网络认证；

本发明将通过优选的实施例结合附图加以说明，但本发明的内容不仅限于实施例中所涉及的内容，其中：

图 1 是识别卡及其结构逻辑图。

图 2 是人体生理特征采集装置及其功能逻辑图。

图 3 是人体生理特征压缩装置及其功能逻辑图。

图 4 是人体生理特征加密装置及其功能逻辑图。

图 5 是人体生理特征密码流储存过程图。

图 6 个人财务帐单、个人档案等信息储存过程图

图 7 是人体生理特征解密装置及其功能逻辑图。

图 8 是人体生理特征解压缩装置及其功能逻辑图。

图 9 是识别卡的鉴别与认证逻辑过程图。

图 10 是识别卡鉴别与认证装置及其功能逻辑图。

图 11 是识别卡及其网络系统逻辑拓朴图。

实施例 1. 某部应用本发明于门卫系统；条件假设(1)门卫已受过人脸图像识别训练；(2)识别卡及网络终端；

1.1 识别卡

如图 1 所示；

1.1.1 采用 IC 卡基的识别卡

识别卡采用 IC 卡基并符合 IC 卡标准 ISO/IEC7816;

1.1.2 采用 LC 卡基的识别卡

识别卡采用 LC 卡基并符合 LC 卡标准 ISO/IEC11693 和 ISO/IEC11694;

1.1.3 复合卡

将 IC 芯片集成在同一张 LC 卡上形成复合卡;

1.2 人体生理特征采集

在识别卡初始化前,发卡机构实时采集识别卡申请自然人或法人的人体生理特征。

1.2.1 人脸图像采集

如果这个过程用数码像机及其附属设备完成,则只需将数码像机所采集的人脸图像数码流通过专用或通用传输装置,传输至电脑中;电脑利用符合联合图片专家组标准的静止图像压缩算法(JPEG),对人脸图像数码流进行压缩处理至 1K 人脸图像数码压缩流;随后用符合国际数据加密标准的对称密码体制数据加密算法对该图像文件进行加密处理,所得到的图像密码流即作为写识别卡的数据;例如图 2、图 3、图 4 和图 5 所示。

1.2.2 指纹采集

使用活体指纹采集装置实时采集人体指纹数码流,再用数码压缩装置将其压缩处理成 0.3K 字节人体指纹数码压缩流,经对称密码体制数据加密算法将其加密处理成人体指纹密码流;例如图 2、图 3、图 4 和图 5 所示。

1.2.3 人脸图像和指纹密码流储存

将上述所得人脸图像密码流和指纹密码流写入 IC 卡内存储器或 LC 卡内存储层;如图 5 所示。

1.3 门卫认证

当持卡者通过门禁系统时,将所持识别卡插入识别卡终端后,将手指按在活体指纹采集装置上,认证过程开始:(1)门卫通过眼睛认证屏幕所显示该识别卡所存人脸图像与持卡者人脸图像是否相符?(2)指纹认证装置核对与认证:识别卡内所存指纹与活体指纹装置所采集到的指纹是否相符?(3)当上述认证结果符合要求则准其通过并完成认证过程。

（实施例 2. 某银行应用本发明于金融卡系统；条件假设：(1)用户群多达一千万以上；(2)已有分布式识别卡网络；(3)已有连网或脱机特约金融卡服务网点；如图 11 所示；

2.1 识别卡

如图 1 所示；

2.1.1 采用 IC 卡基的识别卡

识别卡采用 IC 卡基并符合 IC 卡标准 ISO/IEC7816；

2.1.2 采用 LC 卡基的识别卡

识别卡采用 LC 卡基并符合 LC 卡标准 ISO/IEC11693；

2.1.3 复合卡

将 IC 芯片集成在同一张 LC 卡上形成复合卡，并符合上述有关识别卡标准；

2.2 人体生理特征采集

在识别卡初始化前，发卡机构需要采集识别卡申请自然人或法人的人体生理特征信息，并建立申请人财务帐单；

2.2.1 人脸图像采集

如果这个过程用数码像机及其附属设备完成，则只需将数码像机所采集的人脸图像数码流通过专用或通用传输装置，传输至电脑中；电脑利用符合联合图片专家组标准的静止图像压缩算法 (JPEG)，对人脸图像数码流进行压缩处理至 1K 字节的人脸图像数码压缩流；随后用符合国际数据加密标准的对称或非对称密码体制数据加密算法对该图像文件进行加密处理，所得到的图像密码流即作为写识别卡的数据；例如图 2、图 3、图 4 和图 5 所示。

2.2.2 指纹采集

使用活体指纹采集装置实时采集人体指纹数码流，再用二值图像数码压缩装置将其压缩处理成 0.3K 字节人体指纹数码压缩流，经对称或非对称密码体制数据加密算法将其加密处理成人体指纹密码流；例如图 2、图 3、图 4 和图 5 所示。

2.2.3 手几何形态采集

使用活体手几何形态采集装置实时采集人体手几何形态数码流，再用二值图像数码压缩装置将其压缩处理成 0.6K 字节手几何形态数码压缩流，经对称或

非对称密码体制数据加密算法将其加密处理成手几何形态密码流；例如图 2、图 3、图 4 和图 5 所示。

2.2.4 人脸图像密码流、指纹密码流和手几何形态密码流储存

将上述所得 2K 字节的人脸图像密码流、指纹密码流和手几何形态密码流写入 IC 卡内存储器或 LC 卡内光存储层；如图 5 所示。

2.2.5 个人财务帐单

将个人财务信息如存款余额、流水帐、最大允许透支额、信用等级等信息经数据压缩算法和数据加密算法处理成密码流后存储入识别卡中；如图 6 所示。

2.3 金融服务

识别卡服务原则 1：识别卡接受任何金融服务请求时，都必须鉴别与认证持卡人人体生理特征后进行；

识别卡服务原则 2：识别卡接受识别卡终端操作命令时，只对识别卡中个人财务帐单所涉金融余额和最大允许透支额作相减操作，且不允许负数操作；

识别卡服务原则 3：识别卡接受发卡行操作命令时，除包含上述原则 1 和原则 2 外，还允许进行其它操作；

2.3.1 刷卡时金融卡终端服务过程

如图 9 所示；

(1)金融卡终端接受刷卡者刷卡请求，首先查验该卡有效性，然后实时采集持卡人人体生理特征数码流并向金融卡发出正当性鉴别请求并将失效卡名单传至金融卡；

(2)金融卡接受金融卡终端正当性鉴别请求与失效卡名单后，按约定鉴别金融卡终端的身份，只有当金融卡与金融卡终端相互正当性身份鉴别准确无误完成，金融卡才允许金融服务过程继续，否则终止金融服务；若该金融卡被列入失效卡名单则本卡置失效标识并终止金融服务；

(3)金融卡解密和解压缩所存人体生理特征密码流及解密和解压缩所存个人财务帐单密码流；

(4)金融卡接受金融卡终端传输的持卡人人体生理特征数码流，并采用相关匹配法与卡中人体生理特征数码流鉴别与认证：该持卡人是否为合法持卡人？否

则终止金融服务过程；如图 10 所示；

(5)金融卡与金融卡终端对持卡者进行金融服务：提款、消费、结算；金融服务根据发生额对卡中个人财务帐单中金融余额与最大允许透支额进行减操作，发生额必须小于等于金融余额与最大允许透支额；金融服务完成后，金融卡中个人财务帐单将根据发生额实时修改并经压缩和加密处理后写回识别卡；连网时，金融卡终端将发生额及金融卡号、金融卡个人财务帐单传输至网络控制中心；

(6)金融服务终止；

2.3.2 发卡行金融服务

发卡行金融服务过程除包括金融卡终端服务项目外，还允许持卡者要求：更改个人标识信息、修正人体生理特征信息、存款、申请最大允许透支额和查阅个人财务帐单等金融服务；

说明书附图

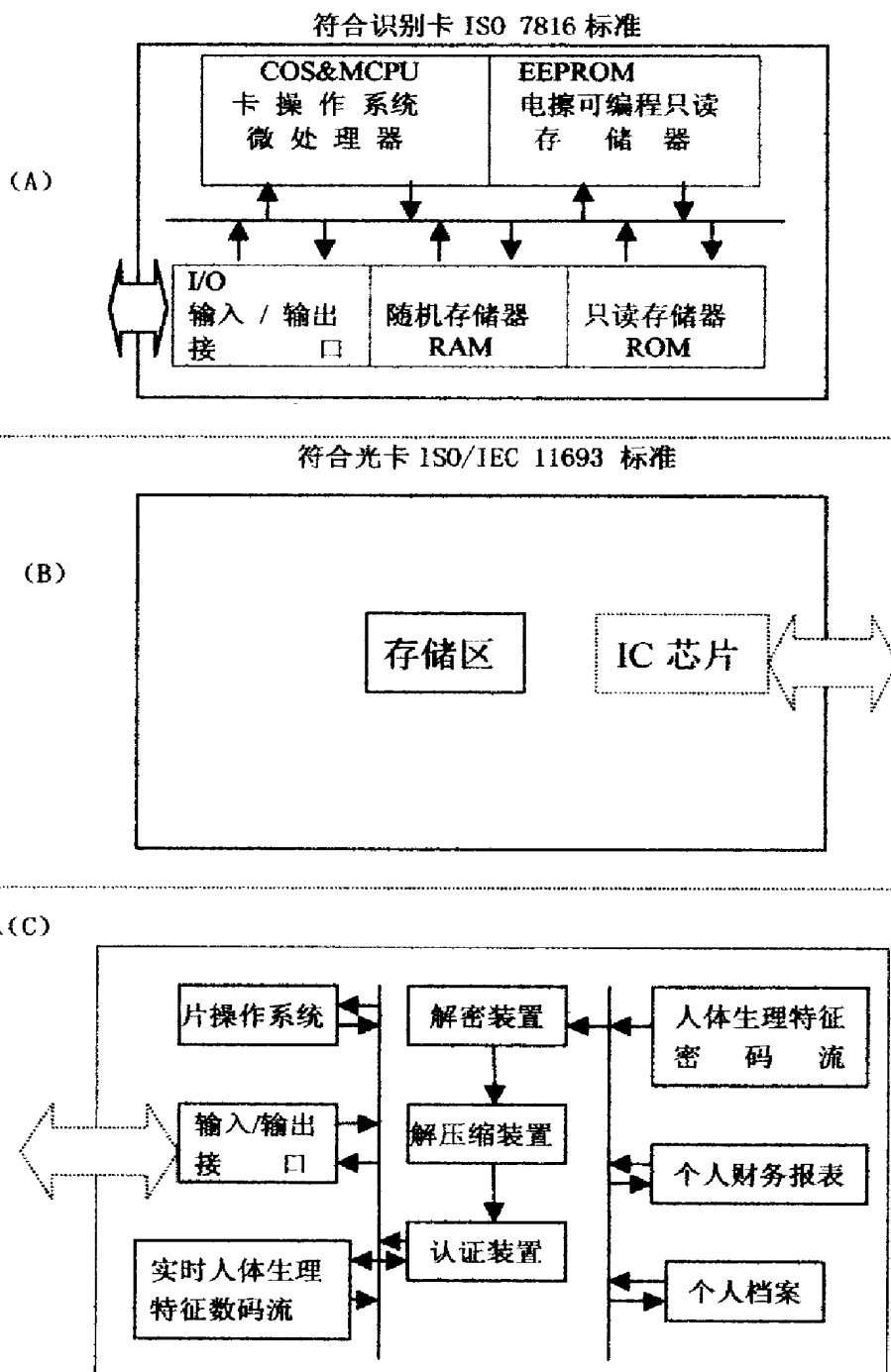


图 1

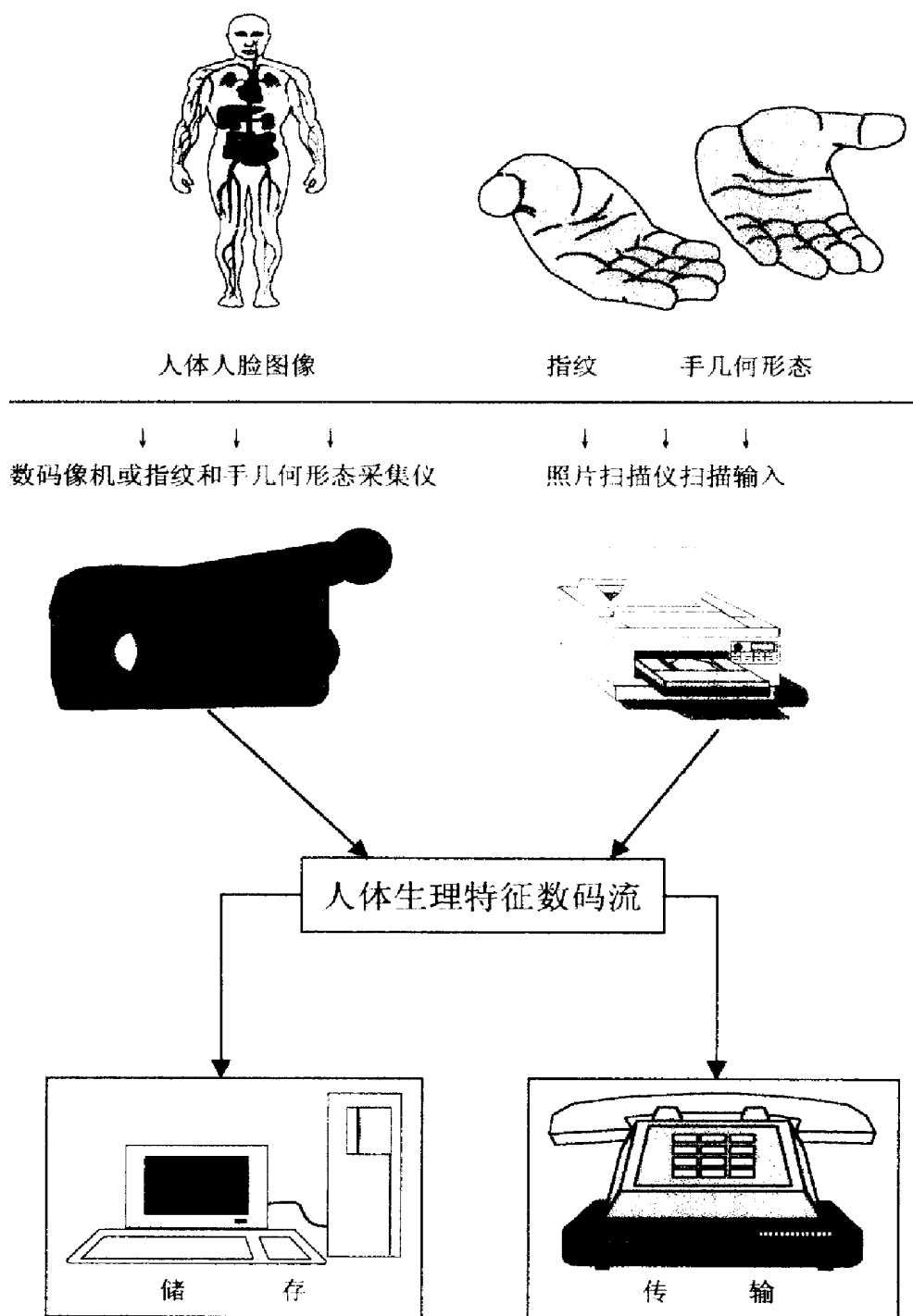


图 2

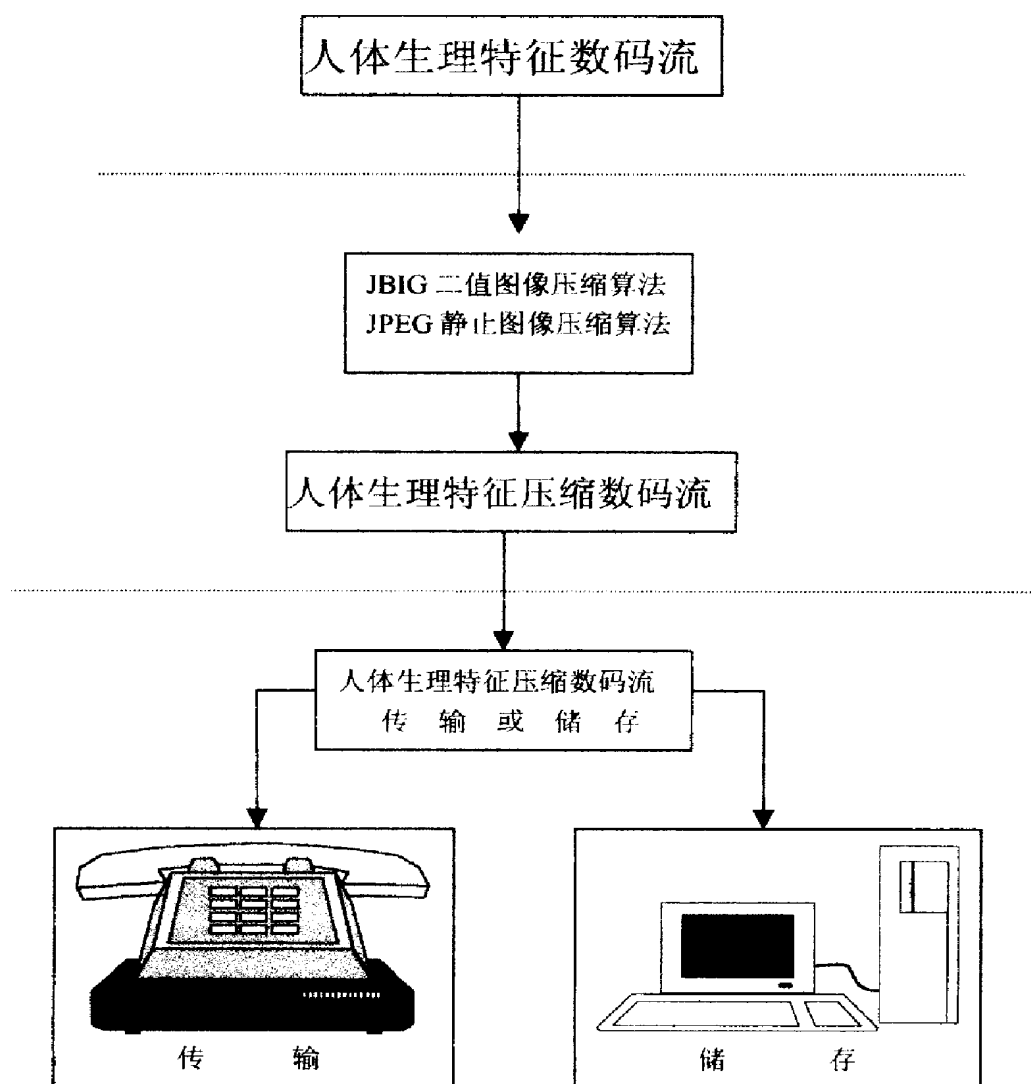


图 3

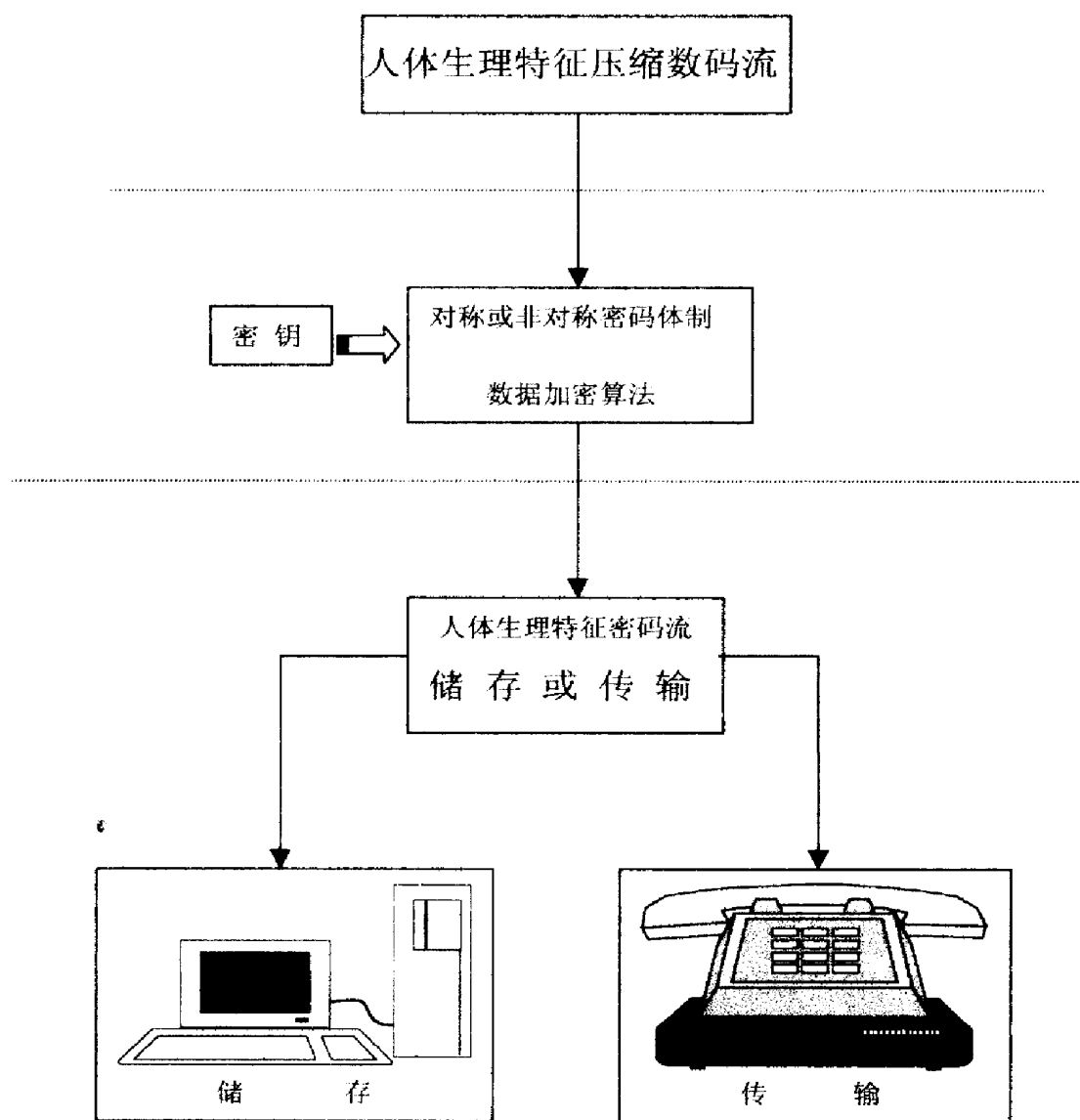


图 4

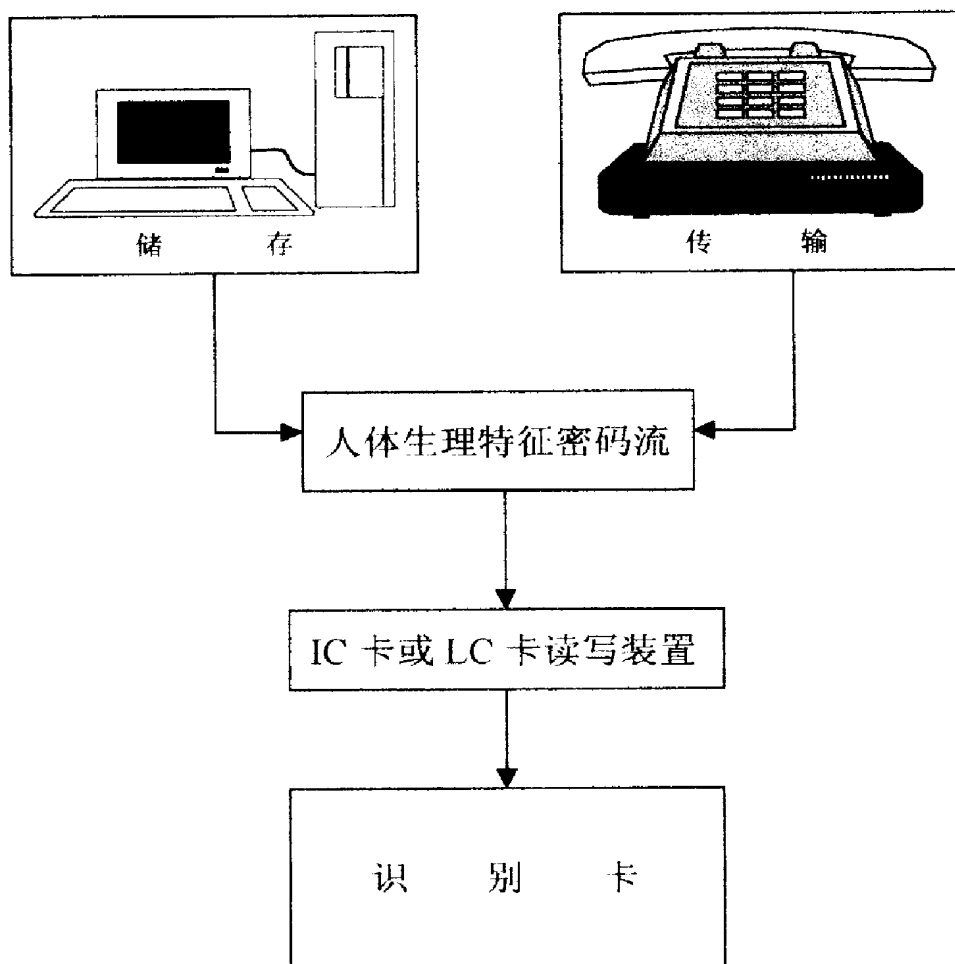


图 5

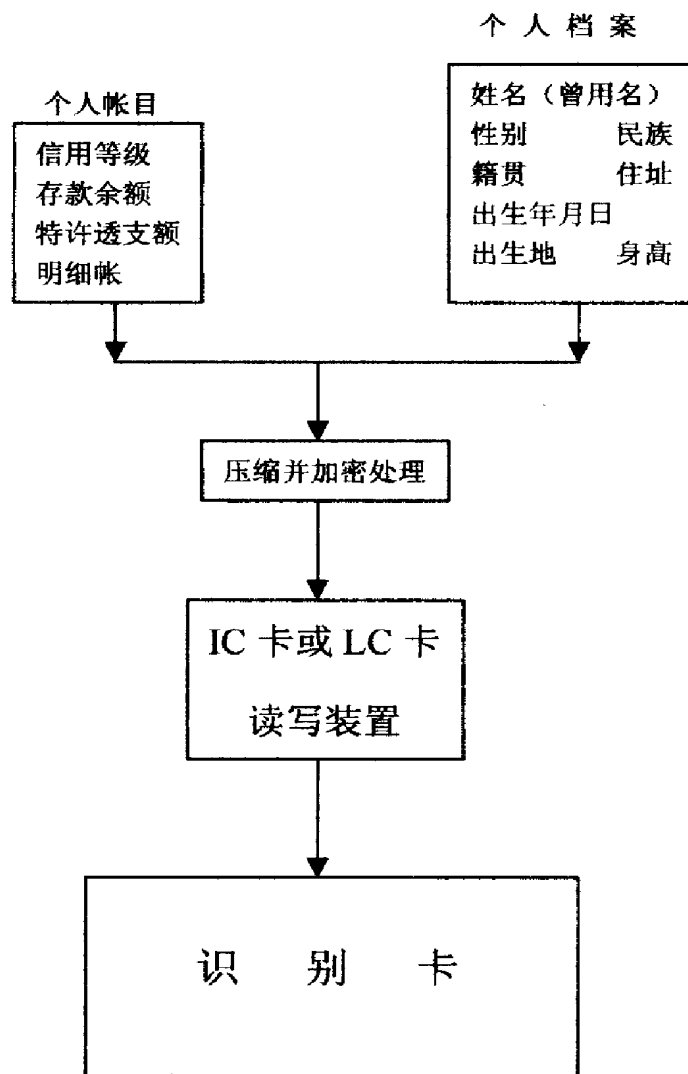


图 6

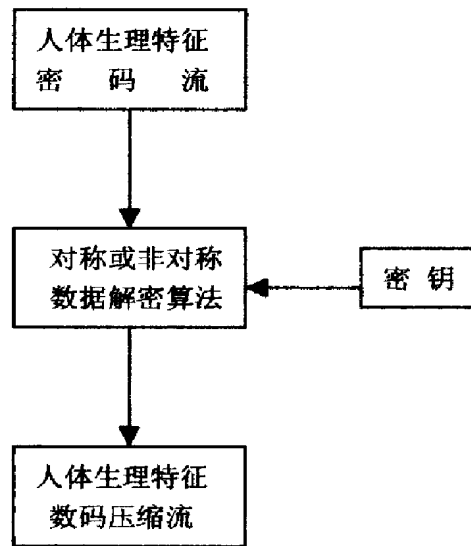


图 7

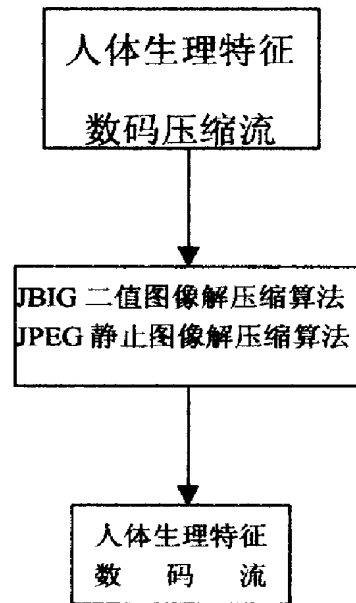


图 8

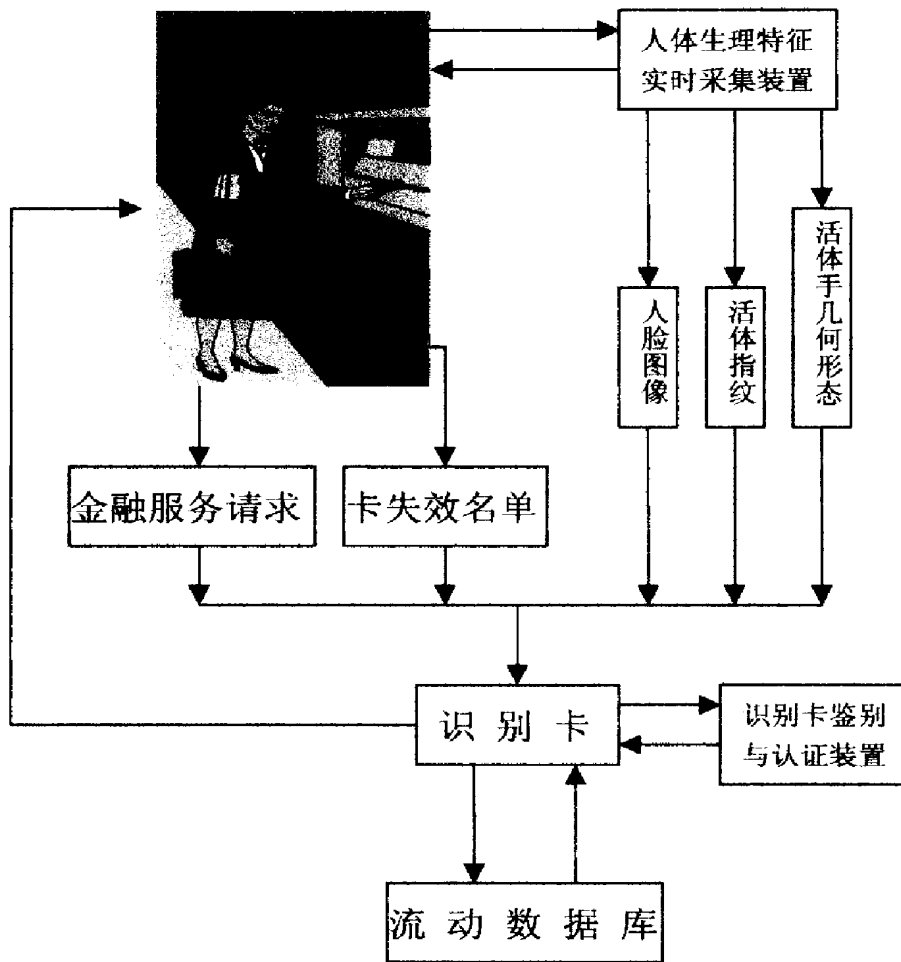


图 9

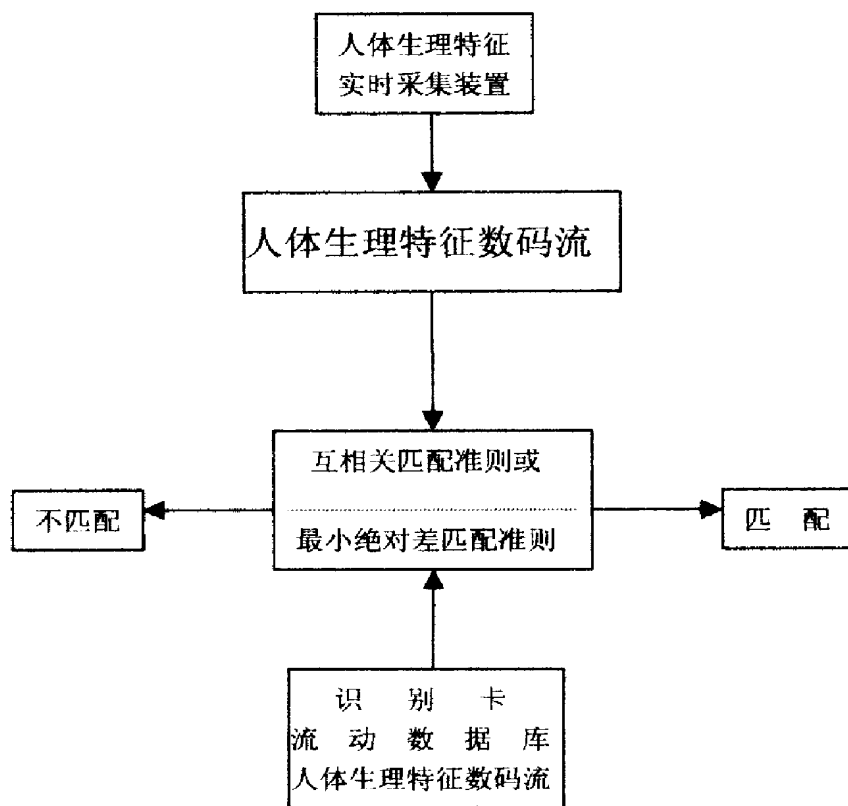


图 10

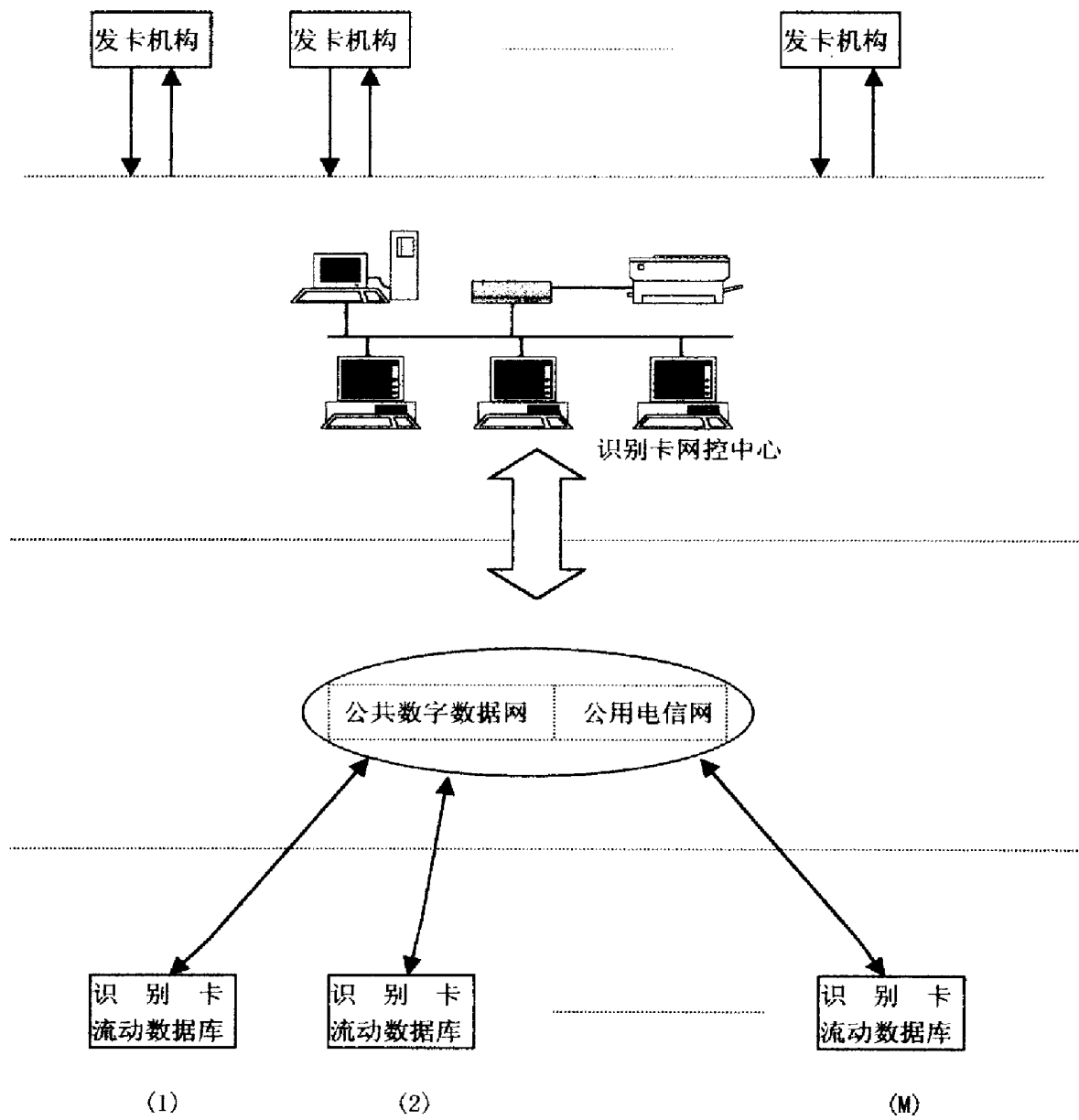


图 11